NAVAL WAR COLLEGE
Newport, RI

CONFRONTING CHALLENGES TO JOINTNESS: INITIATIVES FOR JOINT COMMAND AND CONTROL

by

Jeremiah F. Garretson

Lieutenant Colonel, United States Army

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Operations Department.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: Jeremiah F. Garretson

18 June 1993

Paper directed by
Professor Milan Vego
and
CAPT Micajah W. Newman
Operations Department

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT DISTRIBUTION STATEMENT A: APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION OPERATIONS DEPARTMENT 6b. OFFICE SYMBOL (If applicable) C	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State, and ZIP Code) NAVAL WAR COLLEGE NEWPORT, R.I. 02841	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING / SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10. SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.

11. TITLE (Include Security Classification)

CONFRONTING CHALLENGES TO JOINTNESS: INITIATIVES FOR JOINT COMMAND AND CONTROL (U)

12. PERSONAL AUTHOR(S)
GARRETSON, JEREMIAH F., LTC, USA

13a. TYPE OF REPORT	13b TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
FINAL	FROM _____ TO _____	93 JUN 18	31

16. SUPPLEMENTARY NOTATION A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Operations. The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

17. COSATI CODES		
FIELD	GROUP	SUB-GROUP

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
Command and Control
Interoperability
Defense Information Infrastructure

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

Initiatives that place Command, Control, Communications, Computers, and Intelligence (C4I) systems on a "joint" path are assessed against the JCS "C4I for the Warrior" concept. A basis is made that this concept is a seminal doctrine for command & control in joint operations in that it contains a number of broad operational requirements for C4I systems in support of the CJTF. Also presented are challenges that threaten progress in achieving the objective of "a seamless, secure, interoperable global C4I network for the Warrior." The challenges result from changes in strategic focus that place new demands on C4I systems; from an "ownership" culture reflected in reluctance to give up C4I assets for consolidation and standardization; and from technical interoperability problems. Several initiatives which confront these challenges are examined. DMRD 918, the decision to establish the Defense Information Infrastructure under DISA is of particular interest in that it is the most ambitious step taken toward the interoperable global network. Though the initiatives face significant problems, the momentum toward jointness created by the Goldwater-Nichols Act will cause them to prevail. The C4I system for the Warrior looms on the horizon.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT. ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL CHAIRMAN, OPERATIONS DEPARTMENT	22b. TELEPHONE (Include Area Code) 841-3414 22c. OFFICE SYMBOL C

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted. All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

★U.S. Government Printing Office 1988—539-012

Abstract of
CONFRONTING CHALLENGES TO JOINTNESS:
INITIATIVES FOR JOINT COMMAND AND CONTROL

Initiatives that place Command, Control, Communications, Computers, and Intelligence (C4I) systems on a "joint" path are assessed against the Joint Chiefs of Staff "C4I for the Warrior" concept. A basis is made that this concept is actually a seminal doctrine for command and control in joint operations in that it contains a number of broad operational requirements for C4I systems in support of the Commander, Joint Task Force (CJTF). Also presented are challenges that threaten progress in achieving the "objective of a seamless, secure, interoperable global C4I network for the Warrior." The challenges result from changes in strategic focus (i.e., global conflict to regional crises and contingencies) that place new demands on C4I systems; from an "ownership" culture reflected in resistance to give up C4I assets for consolidation and standardization; and from technical interoperability problems. Several initiatives which confront these challenges are examined. DMRD 918, the decision to establish the Defense Information Infrastructure under the Defense Information Systems Agency is of particular interest in that it is the most ambitious step toward the interoperable global network. Though the initiatives face significant problems, the momentum toward jointness created by the Goldwater-Nichols Defense Reorganization Act of 1986 will cause them to prevail. It may be delayed, but a joint C4I system for the Warrior already looms on the horizon.

TABLE OF CONTENTS

CONFRONTING CHALLENGES TO JOINTNESS: INITIATIVES FOR JOINT COMMAND AND CONTROL

CHAPTER I

INTRODUCTION

Last June, a lofty concept was depicted by General Colin Powell, Chairman of the Joint Chiefs of Staff, in the preface to a booklet titled C4I for the Warrior. Articulated in the concept were broad operational requirements that laid out a "roadmap to reach the objective of a seamless, secure, interoperable global [command, control, communications, computers, and intelligence] C4I network for the Warrior.[1] The goal of this global network is to allow any deploying unit to arrive in theater "and simply plug into the grid or [Defense Information System Network] DISN and automatically obtain service."[2] In this version and in a significant follow up effort to expand upon the C4I for the Warrior concept, the Joint Task Force appropriately is stressed as the focal organization to be supported.[3]

An important step toward transforming the concept into reality was taken with the signing of Defense Management Report Decision (DMRD) 918, The Defense Information Infrastructure, by then Deputy Secretary of Defense, the Honorable Donald J. Atwood, on 15 September 1992. This decision established the Defense Information Systems Agency (DISA) "as the central manager of the defense information infrastructure,"[4] and transferred to DISA several functions, along with trained personnel, equipment, and facilities, that are

currently accomplished by the separate services and defense agencies.

Using General Powell's "C4I for the Warrior" vision as a benchmark goal, this paper examines the operational requirements for C4I systems as a result of the increasing trend in joint military operations; discusses challenges to the achievement of General Powell's vision of a global information grid; and, finally, assesses how well DMRD 918 and other initiatives are confronting these challenges .

CHAPTER II

OPERATIONAL REQUIREMENTS FOR A JOINT C4I SYSTEM

Section 1. The trend to joint military operations

The C4I for the Warrior concept is a natural iteration of the process begun with the enactment of the Goldwater-Nichols Department of Defense Reorganization Act of 1986. Prodded by Urgent Fury (the invasion of Grenada in 1983) which offered a fresh example of barely adequate command and control in joint operations, and the realization that most future military operations would be joint in nature, the act set out to impose changes on a reluctant military establishment.

One need only point to joint military operations occurring after 1986 (e.g., Just Cause, Desert Storm, and Restore Hope) to validate the success of the Goldwater-Nichols Act. However, the presence of seams and barriers in the command and control process has prevented military from realizing the full potential of jointness. This can be demonstrated by a look at the three functions of command and control and their current level of maturity following the mandate to change.

Van Creveld in his book titled Command in War identifies three "unchanging functions" of command. These are: organization, procedures, and technical means.[6] The most immediate impact of the Goldwater-Nichols Act was to "reorganize" the military command and control structure by shifting power from the individual service chiefs to the Chairman of the Joint Chiefs of Staff (CJCS) and the Unified and Specified Commanders in Chief (CINCs). It is with this command and control function that the most significant

change took place. In fact this change dominates and influences the remaining functions of procedure and technical means.

Van Creveld uses the term "procedures" to encompass doctrine, procedures and training. In this context, since 1986, substantial progress has been made to develop a joint schooling infrastructure. Less progress has been made in the development of joint doctrine. One reason: joint schooling is tied to promotion to flag rank, thus giving immediate purpose to implementing educational changes. This partially explains the lag of joint doctrine development. Most likely, the explanation for the lag is the enormous difficulty in getting the separate services, ingrained with their own cultures and philosophies, to agree on joint doctrine.

As a consequence, the immaturity of joint doctrine has limited what can be taught in the schools. For example, most of the joint curriculum focuses on staff procedures and service doctrines instead of joint *operational* doctrine. One critic arguing for a reform of the joint doctrine process aptly summarizes the proper relationship of doctrine and education in the following statement. "Command authority and doctrine, not merely education, cause military forces to function together. Education is simply the mechanism for ensuring the ideas are understood and implemented."[7] This lack of joint doctrine also has retarded the evolution of the remaining function of command, the technical means (C4I systems), toward a joint system.

Now that it has been written, the C4I for the Warrior concept can be interpreted as a broad description of joint operational doctrine. Operational requirements for C4I systems are being derived from the concept and technical means have begun their

evolution to jointness. The fact that the concept's proponent is the CJCS establishes it as a seminal doctrine from which more elaborate doctrine will emerge. Joint operations and the CJTF have finally become the focus of C4I systems.

Section 2. Operational requirements for the "technical means"

The joint requirements contained in the C4I for the Warrior are actually embodied in "guiding principles" that only lack measurable criteria upon which to develop/acquire the global grid. These "operational requirements" are to provide an integrated C4I system that:

- will support any US force in the accomplishment of any mission - any time and place
- will provide accurate and complete pictures of the relevant battlespace
- will provide a means for any US force to receive timely and detailed mission objectives
- will provide the clearest view of targets
- is interoperable
- is responsive, reliable, and secure

The operational requirements are general, but they serve the purpose of providing the goal for future C4I efforts. More specific C4I operational requirements to improve joint operations can be derived from the Defense Science and Technology Strategy, dated July 1992, produced by the Office of the Director of Defense (Research and Engineering). Table I provides a contrasting list of examples of today's C4I capabilities and those that advancing technology will make possible tomorrow. These "potential" capabilities are

consistent with the C4I for the Warrior concept. The roadmap has been drawn and the journey started; however, obstacles in the form of challenges are in the way.

Table I. Examples of C4I capabilities that will improve joint operations and which will be made possible by advances in technology. *Source: Defense 92, November/December.*

Today	2000-2005: Potential
Global Surveillance and Communications	
o Separate systems - segregated tasking by system - restricted area coverage - limited flexibility in mission, sensors and reference data	o Integrated systems with expanded broad area sensing - integrated tasking - precision, all-weather sensing through mission assessment for multiple missions - access to extensive reference data
o Independent communications networks and systems with ad hoc interconnects - limited capacity - independent data services	o Very high capacity backbone - interoperable across ground, sea, space, and air - multimedia services - multilevel security
o Barriers between operations and intelligence	o Seamless flow of intelligence
o Limited surge - Independent systems command and control, planning	o Rapid surge, deployable worldwide - "system of systems" operating on a global grid - integrated systems command and control, planning, simulation
Precision Strike	
o Cumbersome joint strike/mission planning - sensor/weapon retasking unwieldy - slow dissemination of surveillance data/ imagery, intelligence and force orders	o Joint quick-reaction kill of time-sensitive targets - dynamic sensor/weapon retasking o Interoperable, timely, on-demand dissemination to operators
Air Superiority and Defense	
o Autonomous weapon systems	o Netted systems providing: - optimal resource allocation - cooperative engagement
Advanced Land Combat	
o Voice radio, paper maps, grease pencils	o Burst transmissions, electronic maps/automated crew functions, situational awareness/intelligent decision aids

CHAPTER III

CHALLENGES TO THE VISION

Section 1. Strategy and irony

The shift in focus from potential global conflict to regional contingencies, military down-sizing, and defense budget cuts have driven changes in the National Military Strategy (NMS). These strategic changes are revealing the shortfalls in the infrastructure used to support and sustain fighting forces in the manner to which we have become accustomed.

The end of the Cold War has created a situation resulting in a serious irony. The lessening former-Soviet threat is being met with a draw down of US forward-deployed forces and the closure of bases overseas. At the same time, the relaxing of bipolar tensions has unleashed deep nationalistic, ethnic, religious and other enmities previously suppressed by Cold War tensions. The threat of global annihilation has been replaced with the reality of regional instability.

Consider three of the strategic foundations to the NMS. The foundation of *forward deployment* has been replaced by *forward presence*. Currently, *forward presence* is fairly robust because it includes forward deployed operational forces now released from Cold War dedicated threats. As the draw down continues, it will become less so. More significantly, regional instability has given greater importance to *crisis response* and down-sizing has prompted the addition of *reconstitution* as a strategic foundation.

Yet it has been our reliance on *forward deployed* forces and infrastructure that

enhanced our ability to respond to crises and sustain forces during contingencies. For example, EUCOM provided forces and lent its infrastructure (e.g., theater intelligence facilities, theater command and control network, and operational/logistical staging areas) in support of CENTCOM during Desert Shield/Desert Storm. EUCOM also conducted Provide Comfort (Northern Iraq) and Provide Hope (emergency aid to CIS). As overseas infrastructure continues to shrink, it will be necessary to respond to crises and support them from the United States (e.g., Restore Hope - Somalia).

This is the crux of a military readiness irony: down-size and draw back because the Cold War is over (create the "Peace Dividend"); maintain readiness and respond more frequently to regional crises no longer suppressed by Cold War tensions. The momentum of the Peace Dividend has resulted in the loss of overseas infrastructure that probably is irreversible. Therefore, it stands to reason that our ability to respond to crises and contingency operations on a unilateral basis will be less flexible at a time of more frequent occurrence. As far as providing a C4I support structure to meet this challenge, a new approach is needed.

We cannot rely upon the shrinking and less capable infrastructure of overseas land based telecommunications (i.e., DISN) and information networks that are bridged by limited capacity satellite and undersea cable telecommunications systems. Even if it remained in its present state, this Cold War "designed" communications/information infrastructure is inadequate to support regional contingencies outside of PACOM and EUCOM. To restore flexibility to *crisis response* in the area of command and control, future C4I systems must accommodate the principles of strategic agility and power

projection. These principles are supported in the global information grid envisioned in C4I for the Warrior.

Section 2. Cultural obstacles

Perhaps the greatest obstacles to overcome in order to achieve the C4I for the Warrior vision are the divergent "ownership" cultures of the separate services and agencies. These cultures had a headlock on C4I systems that is slowly being loosened as joint operations reveal shortcomings. "Deficiencies in joint C2 stem primarily from an enduring legacy of service compartmentalization."[8] "Current C2 systems are the heritage of years of largely unplanned splicing together of ill-fitting components that were delivered to the service elements of joint forces by relatively independent parties far away, who coordinated adequately neither with the joint commanders nor with each other."[9]

Ironically, the Goldwater-Nichols act added the CINC as an "ownership" obstacle. CINCs have had at their disposal data processing facilities and software design activities that allowed them to develop unique information systems to train, administer, and support during peacetime operations. This caused costly redundant efforts, created information systems that cannot interoperate with each other, and exposed operational data to information exploitation by friendly and unfriendly agents. Figure 1 depicts the

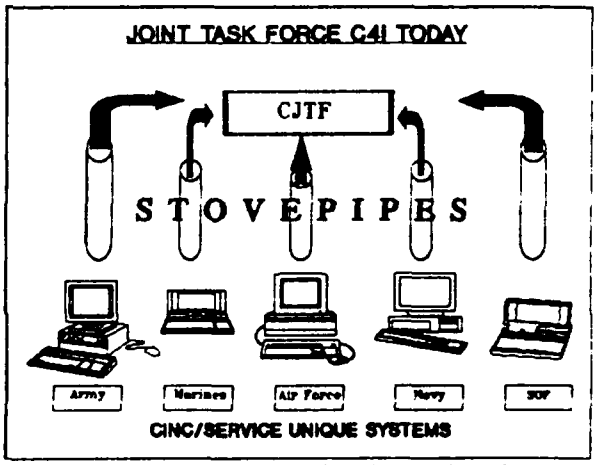

Figure 1. A depiction of today's situation regarding information systems. *Source: C4I for the Warrior.*

situation a Joint Task Force commander would face today with information systems as a result of the service/CINC ownership cultures.

This situation is replete with barriers and seams that prevent the sharing of information at levels lower than the CJTF. It also creates an environment where the CJTF must simultaneously view four or five displays and serve as the system integrator.[10] A corollary to this problem is that the CJTF becomes inundated with information and must disseminate "joint" information back down the stovepipes. A bottleneck develops that chokes the efficiency and effectiveness of the command and control process.

The new vision for C4I systems will eliminate this situation which is a manifestation of the culture that placed service and CINC requirements above joint requirements. Instead of multiple displays, the goal is that one day the CJTF will have a single display for all battle space information.

Section 3. Technical obstacles: seams, barriers, and interoperability

Interoperability is an unusual term within the military lexicon. In the context of C4I systems, it is "the condition achieved when information or services can be exchanged directly and satisfactorily."[11] Unfortunately interoperability is also relative. To be interoperable many systems require translation devices or special interfaces and often must compromise their operational capability. For example, the Army has developed an extremely capable combat net radio called SINCGARS. Because of its operating characteristics (i.e., frequency hopping and advanced security algorithm) it is resistant to jamming, intrusion, and interference.

It is considered interoperable with tactical radios of other services operating in the

same frequency band. It also is "interoperable" with allied tactical radios such as Britain's JAGUAR (frequency hopping) and Germany's FUGAR (frequency scanning). However, the systems are only interoperable in the single channel, non-secure mode. Each gives up the vulnerability protection inherent in the frequency hopping/scanning mode when used to pass information between them. This is an example of a seam that prevents the systems from operating to full potential in the joint or combined environment.

Barriers are most common in the functional area of automation. They prevent the flow, transfer, or sharing of information. When he was J-6, VADM Macke observed that, "the technology explosion in information systems hardware and software has provided an enormous capability to aid combat commanders on the battlefield. Innovative commanders and their support elements have jumped on this phenomenon to fabricate a wealth of devices."[12] The desire to get the new technology to the field resulted in a lack of coordination between "inventors and developers" and, most importantly, among the users. As a consequence, a number of "worthwhile but stand-alone products" exist in a unique command environment and do not lend themselves to joint operations.

Interoperability problems in the form of seams and barriers were subdued by the enormous success of the C4I effort during operations Desert Shield and Desert Storm. But clues to problems can be found. For example, in lauding the C4I effort, the Interim Report to Congress on the Conduct of the Persian Gulf Conflict states the following, "US, Coalition, and commercial communications assets were employed to support deployment, sustainment, and combat operations. All of this required considerable innovation. [my

underline for emphasis]"[13] The seams and inadequacies were apparent in the necessity for numerous innovations to adapt or tie into other C4 networks.

The seams and barriers were manifested in operational problems. Though the C4I system developed by CENTCOM supported an overwhelming amount of data, the data was often too much to absorb, was misdirected, or redundant. Additionally, the proliferation of computers with a variety of application programs and data bases presented training problems among the different organizations. Each system tended to have unique requirements that demanded tailored training programs to be developed and administered by the unit, staff section, or directorate to which the system belonged.[14]

Perhaps the most cited example of a barrier to information transfer was the Air Tasking Order (ATO). Though the Air Force managed targets for air assets of all component commands through a central data base, it was not possible to distribute the ATO in the most efficient manner - electronically. In fact, ATOs were flown out to ships in order to reach the Navy air wings. This manual information transfer sometimes took three days vice the minutes it would have taken electronically. In addition, once it was received the huge document had to be manually scanned to identify the tactical assignments relevant to a particular air unit. Had it been possible to establish a local area network off the Air Force ATO system, with each air element provided a workstation, the power of automation would have saved additional time and energy.[15]

The challenges to achieving the C4I for the Warrior vision are tremendous: the shrinking overseas command and control infrastructure; the increase in regional instability to which military solutions, that rely on the infrastructure, are applied; the culture that

produced stovepipe C4I systems; and the widespread use of systems that lose much of their effectiveness in the joint environment are a few. Another major challenge is a shrinking defense budget that has supplanted the threat as the major influence on strategy development. A consequence might be the failure to achieve a joint C4I environment. The next section discusses recent initiatives to overcome these challenges and make the C4I vision of the future a reality.

CHAPTER IV

CONFRONTING THE JOINT C4I CHALLENGES

Section 1. The initiatives

The challenges are being met with the two initiatives already mentioned (C4I for the Warrior and DMRD 918) and which are the primary focus of this paper. However, two other initiatives should be mentioned as they precede or complement the effort to make C4I systems joint. Several years ago, DMRD 968 was implemented to consolidate DoD long-haul (telecommunications) networks into the Defense Information Systems Network (DISN). DMRD 918 is an expansion of the consolidation effort.

The other initiative is called the Corporate Information Management (CIM) program. The concept of CIM is simple. It recognizes the diversity and age of DoD information assets. It recommends the investment of about $4.5 billion a year over seven years to modernize information systems. It then assumes recoupment at the rate of 20 to 30 percent by the fourth year. In all, it is estimated that for every $1 invested in modernization, $7 will be saved in overhead costs.[14] CIM and DMRD 918 apply to approximately 1700 data processing installations (DPIs), over 38 major central design (software) activities (CDAs), and over 650,000 personal computer (PC) workstations within DoD.

Section 2. DMRD 918

The issue addressed by DMRD 918 encompasses the problems created by heterogenous C4I systems and the positive goal established by the C4I for the Warrior

concept. Equally important, and perhaps its main selling point, is that it addresses wasteful and expensive practices of non-joint C4I systems development and acquisition. Its approval means that the defense information infrastructure will be "managed through central technical control and configuration management with decentralized execution to assure end-to-end information transfer capability which is protected, interoperable, and cost effective."[17]

To understand the scope of DMRD 918, it is important to define what it applies to and what it does not. Figure 2 lists those departments and agencies whose assets form the National Communications System (NCS).[18] The dominant portion of the NCS is owned and operated by DoD whose Defense Communication System (DCS) makes up 80 percent of the NCS. DMRD 918 applies only to the DCS.

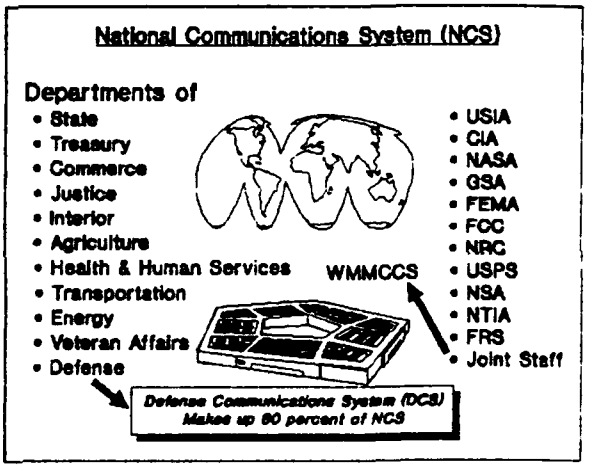

Figure 2. The major departments and agencies that make up the National Communications System (NCS). *Source: Joint Pub 6-0.*

Though many believe the DCS focuses on the strategic level of war, it actually plays a significant combat support role at the operational level by providing C4 services down to the post, camp, and station. At this level, "tactical interfaces" at fixed switching centers and technical control facilities allow major forces (e.g., Army Corps) access to the network.

It is a "heterogenous mixture of systems and facilities independently developed,

supported, and operated by the Commanders of Unified and Specified Commands, Services, Component commands, and Agencies" that provides long-haul, point-to-point, and switched network telecommunications to meet the command and control needs of the DoD and other agencies concerned with national security.[19] It is the intent of DMRD 918 to make the system more homogenous. However, its focus is on the DoD automation systems that provide the bulk of information services (i.e., DPIs, CDAs, and PCs). Outside the scope of DMRD 918 are the following C4I means:

- command and control systems integral to weapons systems
- tactical communications systems
- weapons systems software
- wargaming/simulation
- software support for command and control
- intelligence activities

Section 3. Defense Information Systems Agency and DMRD 918

DISA, as the appointed central manager of the defense information infrastructure, will be responsible for seven functional areas that confront the challenges to a joint C4I system at the operational/strategic and strategic levels. A short discussion of the functional problems and the new DISA responsibilities are contained in the following paragraphs.

Security. Technology and the demand for it have advanced too quickly for security to keep up. The increased use of data bases and computer networking coupled with inadequate security considerations have made information systems vulnerable to a

variety of threats (e.g., unauthorized intruders, viruses, etc.). A nightmarish situation has been created for commanders sensitive to the effective employment of OPSEC procedures. DISA is now responsible for providing funding to support enhanced information security protection and is the DoD focal point to oversee the application of security protection.[20]

Information Technology (IT) Standards. DISA already possesses an IT Standards Program Office. However, it only partially addresses the areas of information transfer, information processing, and command and control standards. The lack of interoperability within DoD has been attributed to this shortfall. DISA now is responsible for applying standards that will accelerate the transition to commercial and Federal Information Processing Standards. The goal is to achieve an open systems environment that encourages interoperability.

Communications. Consolidation of long-haul communications into the DISN was an incomplete solution. The services and defense agencies still maintained separate and unique long-haul networks in addition to the common user voice and data networks which make up the DISN. This has fostered a fragmented approach to "modernizing base level communications, and integrating these systems into a fully interoperable and secure information infrastructure."[21] The result is a patchwork growth of differing systems which introduce new seams and barriers. To correct this problem, personnel involved in network management and control standards will be assigned to DISA. This will ensure base-level systems are integrated under one standard.

Computing. The majority of DoD's DPIs and distributed automation systems (i.e., PC workstations configured in local or wide area networks) do not integrate with each

other or the communications network. This problem is the product of unique CINC and component commander requirements (remember the "ownership" culture). The agreed solution is to let DISA assume responsibility for central management, workload control, systems engineering, technical cross-functional integration centers, standards and planning for DPIs. CINC and service assets performing these functions will transfer to DISA.

Central Design Activities (CDAs). In the past, specific groups and organizations within the military departments and defense agencies have pursued autonomous development and maintenance of software applications. This resulted in duplication of functional software, inefficient use of highly technical resources, and formation of another barrier to open-system architecture within DoD. CDA assets and personnel associated with software design development, reengineering, maintenance, systems integration and common support activities will transfer to DISA.

Acquisition. It was found that separate procurement activities among the services and agencies "operate individually in support of specialized requirements."[22] Similar to problems in other areas, this situation allows duplicate efforts in functional software, and "perpetuates an organizational culture where technology upgrading and associated savings are difficult to achieve."[23] The solution is to assign acquisition (information technology and components) assets and personnel to DISA. The approach to provide automation and software support to users will be on new procurement, selected existing support contracts, leases where economically feasible, reutilized information technology equipment, and existing and emerging software repositories. In short, DISA will become a one stop shopping center to meet automation, networking and software requirements, regardless of

their uniqueness or common use.

Education. It is recognized that DoD's education and training infrastructure needs to be developed. Parallel to this is the strengthening of DoD's career development in communications and automation fields. These actions are necessary to deal effectively with new technologies and changing skill requirements.[24] The ASD (C3I) will determine how information technology education and training are centralized. An approach has been laid out (e.g., ASD (C3I) will appoint an agent to develop training standards, etc.) to meet this challenge, but the solutions remain to be found and implemented.

Section 4. Concerns and resistance

The consolidation of functions at DISA will result in the transfer of over 20,000 personnel by this summer. The potential move of an additional 25,000 will complete the transfer goals of DMRD 918. The process has sent ripples throughout DoD down to the users of information technology assets. Despite the merits of consolidating information technology assets into one defense information infrastructure, some anxiety from the Unified and Specified CINCs has led to concerns and some resistance.

The anxiety may stem from the belief that consolidation will distance the supported commands from elements that used to provide tailored support. Although the CINCs will possess operational control of all information technology assets within their respective theaters, the service "stovepipes" are being replaced by a "super stovepipe" (i.e., DISA) that reports to JCS vice CINC level. This could be perceived as a degradation of support. An uncomfortable feeling shows through in the comments from various CINCs to the DISA plan to implement DMRD 918. These comments actually

resemble concerns of the supported commands; for example, the following were extracted from three Joint Staff (J-6A) compilations of CINC and Service comments dated 13 Jan 93, 12 Feb 93, and 6 Apr 93:

- Customer service: "it is not clear that there will be feedback mechanisms to ensure customer concerns are met."
- Customer service: "customer service would be better placed in an operations (J-3 type) organization where operations are managed in order to preclude separation of customer service from operational reality."
- Operational support: "responsibilities of DITSO [a subordinate organization of DISA] do not address support to the CINCs."
- Operational support: the primary focus should be "on the Joint Task Force mission."
- Command relationship: "what will be the command relationship of DISA organizations providing contingency support to a CINC?"
- Operational support: "how will CINC priorities be established and funded? Both the CINC and Service involvement is essential to ensure proper balancing and levels of support."
- Cost: "will CINCs be allowed to contract for cheaper services?" [Note: this is in response to the new requirement that customers will pay DISA for its services.]

This last bullet adds insult to injury. Supported commands and agencies will be required to pay for information services. While this may not be new in the Navy, it is a

dramatic change in the way business is done in the Army. Several years ago, a similar proposal called Chargeback was never implemented because of resistance from Army component commanders.

The CINC concerns are valid. Equally valid is the need for a central bureaucracy to force interoperability within DoD. The initial price may be responsiveness and compromises in theater unique requirements; the potential return is a network of common utility and the realization of the C4I for the Warrior concept. VADM Macke states, "Existing systems that provide the ability to exchange information through the joint architecture may not satisfy all the command, control, communications, and computer requirements of the definition of what the warrior needs, but they will provide a better capability on a joint and combined battlefield."[25]

The factor that has not been voiced by the CINCs is the one that can cause the most damage by undermining DMRD 918; that is lack of funding. Budget cuts in defense reduced and may eliminate money needed for the CIM program (i.e., modernization and standardization of automation assets). Without being able to standardize information technology assets, DISA will merely inherit disparate functioning DPIs and office automation networks that still cannot interoperate and are expensive to operate and maintain. The advertised savings of $12 billion from DMRD 918 over a period of six years will not occur without the CIM investments. The results of failing to achieve DMRD 918 interoperability and cost saving goals will be a loss of credibility, partial fulfillment of CINC concerns about degraded C4I support, and a delay in achieving the C4I for the Warrior concept.

CHAPTER V

CONCLUSIONS

The Goldwater-Nichols Defense Reorganization Act was a positive shove toward jointness. Since its enactment in 1986, there has been a shift in operational focus from Component Commanders to the Commander Joint Task Force (CJTF). A case can be made that the seminal doctrine for the "technical means" of command and control in support of the CJTF is embodied in the "C4I for the Warrior" concept.

The concept is a source of broad operational requirements for C4I systems that will allow any unit in any location to plug into an interoperable, secure, global information network. This system "can improve the joint warfighter's ability to manage and execute crisis and contingency operations and provide a means for unifying the many heterogenous Service C4I programs currently being pursued."[26]

As in any endeavor responding to change or causing it, there are a number of challenges. One challenge to the joint C4I concept results from the end of the Cold War. The ensuing military draw down is removing the overseas command and control infrastructure that has been relied upon to support military responses to an increasing number of regional crises. The loss of this infrastructure is irreversible. The C4I answer to this lost capability must address jointness, strategic agility, and power projection. The global grid envisioned in C4I for the Warrior does this; and the operational urgency for the global grid is compelling.

However, countering this urgency is a challenge in cultural form that equates

responsibility with ownership. Service, agency, and CINC "ownership" cultures fostered an environment that created "stovepipe" C4I systems that imposed seams and barriers to effective information flow. This situation is expensive, overwhelms the CJTF with information (e.g., multiple displays from each service component), and forces him to be an information integrator and disseminator. Fortunately, the C4I for the Warrior concept is being pushed by the Chairman of the Joint Chiefs of Staff. This "trump card" relegates serious resistance to cooperative concern.

Hopefully, this means that as C4I systems move toward standardization and compatibility within a homogenous information grid, interoperability problems (the seams and barriers) will disappear. Adaptation, innovation, and extraordinary cooperation should be reduced significantly as the C4I support becomes more transparent to the Warrior.

Top driven initiatives are meeting the challenges to the C4I vision head on. Consolidation of long-haul telecommunications (DMRD 968) and information technology assets (DMRD 918) are major steps to ensure future interoperability, cost savings, and improvements in command and control for CINCs and Commanders JTF.

Though the consolidation of C4I assets under DMRD 918 creates some concern among the CINCs, the real danger lies in the lack of funding. Budget cuts are hampering the investment in information technology modernization that will reduce costs, create a open-system information architecture, and improve service. This situation will undermine the consolidation of information technology assets under DISA by tainting it with the failure to achieve cost saving and improved service goals. The potential consequence is a delay in achieving the global C4I network.

However late we are in arriving, the momentum caused by Goldwater-Nichols is moving us in the right direction - greater capability in joint operations. To paraphrase VADM Macke, "C4I systems will be centralized to ensure interoperability and standardization in the interest of jointness. Unique C4I "desired capabilities" may not be met, but the joint C4I architecture will provide a better capability on a joint or combined battlefield."

ENDNOTES

1. Joint Chiefs of Staff, C4I for the Warrior, J6I, the Joint Staff (Pentagon, Washington, D.C.: 1992), GEN Powell's letter.

2. "Level Communications Funds Meet Force Projection Needs," Signal, March 1993, p. 39.

3. This is contained in the expanded version of the JCS C4I for the Warrior, dated 4 September 1992, and still in draft form.

4. Office of the Secretary of Defense, Defense Management Report Decision 918, (Pentagon, Washington, D.C.: 1992), p. 2.

6. Martin Van Creveld, Command in War, (The President and Fellows of Harvard College, 1985), pp. 9-10.

7. Robert A. Doughty, "Reforming the Joint Process," Parameters, Autumn 1992, p. 46.

8. LTG John H. Cushman, "Joint Command and Control," Military Review, July 1990, p. 26.

9. Ibid., p. 32.

10. "Information Exchange Poses Enhanced Warrior Prowess," Signal, June 1992, p. 94.

11. JCS, Ibid. p. 10.

12. Signal, Ibid., p. 92.

13. "Conduct of the Persian Gulf Conflict, an Interim Report to Congress," July 1991, p.15-1.

14. MAJ Michael R. Macedonia, "Information Technology in Desert Storm," Military Review, October 1992, pp. 38-40.

15. There was no physical space to configure ships with the equipment (satellite receivers, automation equipment, etc.) to accomplish this.

16. "Level Communications Funds Meet Force Projection Needs," Signal, March 1993, p. 39.

17. OSD, Ibid., p. 1.

18. "Doctrine for Command, Control, Communications, and Computer Systems Support to Joint Operations," Joint Pub 6-0, (Washington: Joint Staff, J6A), chap. VI, p. VI-1.

19. Ibid., chap. VI, p. VI-2.

20. Diane Hamblen, "Paul Strassmann: Turning Our Upside Down World Right Side Up," Chips, October 1992, p. 8.

21. OSD, Ibid., p. 3.

22. Ibid., p.4.

23. Ibid.

24. OSD, Ibid., p. 5.

25. Signal, Jun 92, Ibid., p. 94.

26. JCS, Ibid., p. 2.

BIBLIOGRAPHY

Coakley, Thomas P. Issues of Command and Control. Washington, D.C.: National Defense University Press, 1991.

Cushman, LTG John H. "Joint Command and Control." Military Review, July 1990, pp. 25-34.

Doughty, Robert A. "Reforming the Joint Doctrine Process." Parameters, Autumn 1992, pp. 45-53.

Hamblen, Diane. "Paul Strassmann: Turning Our Upside Down World Right Side Up." Chips, October 1992, pp. 4-8.

"Honing the 21st Century Technological Edge." Defense 92, November/December 1992, pp. 34-43.

"Information Exchange Poses Enhanced Warrior Prowess." Signal, June 1992, pp. 91-96.

Joint Pub 6-0, "Doctrine for Command, Control, Communications, and Computer Systems Support to Joint Operations." Washington: JCS (J6A), Pentagon.

"Level Communications Funds Meet Force Projection Needs." Signal, March 1993, pp. 37-39.

Macedonia, MAJ Michael R. "Information Technology in Desert Storm." Military Review, October 1992, pp. 34-4.

Office of the Secretary of Defense. Defense Management Report Decision 918 (Defense Information Infrastructure). Washington: 1992

The Joint Staff. C4I for the Warrior. Washington: 1992.

The Joint Staff. Memorandum for the Director, Defense Information Systems Agency, Subject: DMRD 918 Implementation Plan. Washington: J6, 13 January 1993.

The Joint Staff. Memorandum for the DISA Transition Team, Subject: DISA Response to CINC Comments and Questions Concerning DMRD 918 Implementation Plan. Washington: J6, 13 January 1993.

The Joint Staff. Memorandum for the DISA Transition Team, Subject: Communication Implementation Plan for DMRD 918. Washington: J6, 13 January 1993.

Toguchi, MAJ Robert M. and Hogue, James . "The Battle of Convergence in Four Dimensions." Military Review, October 1992, pp. 11-20.

U.S. Department of Defense. Conduct of the Persian Gulf Conflict: An Interim Report to Congress. Washington: 1991.

Van Creveld, Martin. Command in War. The President and Fellows of Harvard College, 1985.